File 348:EUROPEAN PATENTS 1978-2006/ 200617
(c) 2006 European Patent Office
File 349:PCT FULLTEXT 1979-2006/UB=20060427,UT=20060420
(c) 2006 WIPO/Univentio

Set	Items	Description
S1	46358	ENCRYPT??? OR ENCIPHER??? OR CIPHER??? OR SCRAMBL???
S2	21589	S1(3N)(KEY? ? OR METHOD? ? OR METHODOLOG??? OR PROCEDURE? ? OR ALGORITHM? ? OR SYSTEM? ? OR LOGIC OR FORMULA?? OR APPROACH OR MANNER OR MECHANISM? ?)
S3	12518	S1(3N)(TECHNIQUE? ? OR PROCESS OR PROCESSES OR FUNCTION? ? OR SCHEME? ? OR ROUTINE? ? OR WAY? ? OR MODE? ?)
S4	649619	(SECOND OR 2ND OR DIFFERENT OR SEPARATE OR ANOTHER OR OTHER OR ALTERNATE OR ALTERNATIVE)(3W)(KEY? ? OR METHOD? ? OR METHODOLOG??? OR PROCEDURE? ? OR ALGORITHM? ? OR SYSTEM? ? OR LOGIC OR FORMULA?? OR APPROACH OR MANNER)
S5	553953	(SECOND OR 2ND OR DIFFERENT OR SEPARATE OR ANOTHER OR OTHER OR ALTERNATE OR ALTERNATIVE)(3W)(MECHANISM? ? OR TECHNIQUE? ? OR PROCESS OR PROCESSES OR FUNCTION? ? OR SCHEME? ? OR ROUTINE? ? OR WAY? ? OR MODE? ?)
S6	674850	IDENTICAL?? OR DUPLICAT??? OR REPLICA????? OR MATCH??? OR COPY??? OR COPIES
S7	118088	S6(5N)(DATA OR INFORMATION OR CONTENT? ? OR OBJECT? ? OR FILE? ? OR DOCUMENT? ? OR ARTICLE? ? OR TEXT OR AUDIO OR MUSIC OR SONG? ? OR SOUND OR TRACK? ? OR CLIP? ? OR IMAGE? ? OR PICTURE? ? OR GRAPHIC? ? OR VIDEO? ? OR MOVIE? ?)
S8	133091	S6(5N)(SEGMENT? ? OR PORTION? ? OR BLOCK? ? OR SECTION? ? OR PIECE? ? OR PART OR PARTS OR FRAGMENT? ? OR ITEM? ? OR ELEMENT? ? OR PAGE? ? OR WEBPAGE? ?)
S9	177617	S4:S5(10N)(DATA OR INFORMATION OR CONTENT? ? OR OBJECT? ? OR FILE? ? OR DOCUMENT? ? OR ARTICLE? ? OR TEXT OR AUDIO OR MUSIC OR SONG? ? OR SOUND OR TRACK? ? OR CLIP? ? OR IMAGE? ? OR PICTURE? ? OR GRAPHIC? ? OR VIDEO? ? OR MOVIE? ?)
S10	170142	S4:S5(10N)(COPY OR COPIES OR SEGMENT? ? OR PORTION? ? OR BLOCK? ? OR SECTION? ? OR PIECE? ? OR PART OR PARTS OR FRAGMENT? ? OR ITEM? ? OR ELEMENT? ? OR PAGE? ? OR WEBPAGE? ?)
S11	658	S2:S3(50N)S7:S8(50N)S9:S10
S12	328	S1/TI,AB AND S11
S13	71	S1/AB AND S4:S5/AB AND S11
S14	4412	(MULTIPLE OR MULTIPLICITY OR SEVERAL OR PLURAL? OR DUAL? OR VARIOUS)(7W)S1
S15	31	S14/AB AND S11
S16	93	S13 OR S15
S17	36	S16 AND AC=US/PR AND AY=(1978:2002)/PR
S18	36	S16 AND AC=US AND AY=1978:2002
S19	36	S16 AND AC=US AND AY=(1978:2002)/PR
S20	51	S16 AND PY=1978:2002
S21	62	S17:S20
S22	62	IDPAT (sorted in duplicate/non-duplicate order)

22/3,K/29 (Item 29 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00216549
Cryptographic system for a direct broadcast by satellite network.
Verschlusselungssystem fur ein Satellitennetzwerk mit Direktubertragung.
Systeme de cryptage pour une transmission directe par circuit de satellite.
PATENT ASSIGNEE:
GENERAL INSTRUMENT CORPORATION, (264771), 767 Fifth Avenue, New York New York 10153, (US), (applicant designated states: BE;CH;DE;FR;GB;IT;LI;NL;SE)
INVENTOR:
Horne, Donald R., 20 Edgecliff Golfway 403, Don Mills Ontario, (CA)
Jeffers, John M., 141 Shaftesbury Street, 3 Downsview Ontario M3A 5M3, (CA)
LEGAL REPRESENTATIVE:
Allam, Peter Clerk et al (27601), LLOYD WISE, TREGEAR & CO. Norman House 105-109 Strand, London WC2R 0AE, (GB)
PATENT (CC, No, Kind, Date): EP 194769 B1 920506 (Basic)
APPLICATION (CC, No, Date): EP 86301211 860220;
PRIORITY (CC, No, Date): US 710385 850311
DESIGNATED STATES: BE; CH; DE; FR; GB; IT; LI; NL; SE
INTERNATIONAL PATENT CLASS (V7): H04N-007/16; H04L-009/00;
ABSTRACT WORD COUNT: 176

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	EPBBF1	1702
CLAIMS B	(German)	EPBBF1	1664
CLAIMS B	(French)	EPBBF1	1849
SPEC B	(English)	EPBBF1	6403
Total word count - document A			0
Total word count - document B			11618
Total word count - documents A + B			11618

...ABSTRACT A,B), each including a plurality of key fragments, is generated. For each transmission session, **different** sets of **key** fragments may be periodically selected (13) from one of the key blocks and used to **encrypt** the signals (12). Data indicative of the set selection (19) is generated. The key is...

...to each receiver. The set selection data is transmitted to all receivers along with the **encrypted** signals and used to construct the key fragment set for decryption of the transmitted signals. During the transmission session, the **other key** block may be varied to form a replacement key which is distributed to each receiver...

...at one time by selecting a set in the varied key block for use in **encryption** and decryption.

...SPECIFICATION of the decrypted common audio key,is then used to decrypt the audio signal.
An **encrypted** common audio **key** is periodically transmitted to each receiver unit, preferably at least once every transmission session and...

...of a new or replacement common audio key. The replacement key includes a current key **block identical** to that of the previous key and newly varied **key** block. It is **encrypted** and distributed for storage by each receiver unit. At the end of a transmission session, upon command, in the form of a new **encryption key** number indicating a set of fragments from the varied key block for use, all subscriber units switch from one **block** of the common **audio** key to the **other** . Thus, a replacement **key** can be installed without interruption of the operation of the system.

The integrity of the...

22/3,K/30 (Item 30 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

01131622 **Image available**
SYSTEM AND METHOD FOR THE EXCHANGE OF CRYPTOGRAPHIC KEYS
SYSTEME ET PROCEDE D'ECHANGE DE CLES CRYPTOGRAPHIQUES
Patent Applicant/Assignee:
NOKIA CORPORATION, Keilalahdentie 4, FIN-02150 Espoo, FI, FI (Residence), FI (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
RACZ David, 62 Water Street, Winchester, MA 01890, US, US (Residence), US (Nationality), (Designated only for: US)
Legal Representative:
SPENCE Andrew T (agent), ALSTON & BIRD LLP, Bank of America Plaza, 101 South Tryon Street, Suite 4000, Charlotte, NC 28280-4000, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200454167 A1 20040624 (WO 0454167)
Application: WO 2003US38544 20031204 (PCT/WO US03038544)
Priority Application: US 2002314089 20021206
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BW BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE EG ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NI NO NZ OM PG PH PL PT RO RU SC SD SE SG SK SL SY TJ TM TN TR TT TZ UA UG US UZ VC VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL PT RO SE SI SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) BW GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 7075

Fulltext Availability:
Detailed Description

English Abstract
A system for the exchange of cryptographic keys includes a first peer source and a **second** peer **system** . The first peer source is capable of displaying a cryptographic key adapted to at least one of **encrypt** and decrypt electronic information. In turn, the **second** peer **system** capable of capturing the cryptographic key. Advantageously, the **second** peer **system** is capable of capturing the cryptographic key such that a user of the **second** peer **system** is capable of visually confirming receipt of the cr tographic key from the first peer...

...source and second peer source within a field of view of a user of the **second** peer **system** as the **second** peer **system** captures the cryptographic key.

French Abstract
...a l'echange de cles cryptographiques et comprenant une premiere source d'homologue et un **second** **systeme** d'homologue. La premiere source d'homologue est capable d'afficher une cle cryptographique concue pour au moins chiffrer et dechiffrer des informations electroniques. Le **second** **systeme** d'homologue est capable de capturer la cle cryptographique. Le **second** **systeme** d'homologue presente un caractere avantageux en ce qu'il est capable de capturer la...

...et la seconde source d'homologue dans un champ de vue d'un utilisateur du **second** **systeme** d'homologue quand celui-ci capture la cle cryptographique.

Detailed Description
... information. The electronic information can be encrypted and transmitted by one or more devices or **systems** capable of **encrypting** electronic information and transmitting the encrypted information. Similarly, the encrypted information can be received and decrypted by one or more devices or **systems** capable of receiving **encrypted** infonnation and decrypting the encrypted information into electronic information.

In this regard, the encrypted **information** can be decrypted utilizing a **copy** of the cryptographic key when the cryptographic key comprises a private key (privatekey cryptography), or...

...public key (public-key cryptography).

In one embodiment, the second peer system 14 includes a **second** communication **system** 26 capable of encoding electronic **information** with the cryptographic key and thereafter transmitting the encrypted inforination.

Similarly, in one embodiment, the...

22/3,K/31 (Item 31 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

01114176 **Image available**
SELECTIVE ENCRYPTION FOR VIDEO ON DEMAND
CRYPTAGE SELECTIF A LA DEMANDE POUR VIDEO
Patent Applicant/Assignee:
SONY ELECTRONICS INC, 1 Sony Drive, Park Ridge, NJ 07656, US, US (Residence), US (Nationality)
Inventor(s):
CANDELORE Brant L, 10124 Quail Glen Way, Escondido, CA 92029-6502, US,
Legal Representative:
KANANEN Ronald P (et al) (agent), RADER FISHMAN & GRAUER PLLC, 1233 20th Street, NW, Suite 501, Washington, DC 20036, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200436892 A2-A3 20040429 (WO 0436892)
Application: WO 2003US27775 20030908 (PCT/WO US03027775)
Priority Application: US 2002409675 20020909; US 2002273903 20021018; US 2002274084 20021018; US 2002274019 20021018; US 2002273905 20021018
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE EG ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NI NO NZ OM PG PH PL PT RO RU SC SD SE SG SK SL SY TJ TM TN TR TT TZ UA UG UZ VC VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL PT RO SE SI SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 5676

Fulltext Availability:
Detailed Description

English Abstract
A video on demand (VOD) method, consistent with the invention involves storing multipleselective **encrypted** VOD cotnent on a VOD server; receiving an order for the VOD contentspecifying delivery to a target decoder; determining what CA **encryption** system is associatedwith the order; stripping all **encrypted** segments from the **multiple** selectively **encrypted** contentthat are not associated witht he order to produce single selectively **encrypted** VOD content tothe target decoder. The **multiple** selectively **encrypted** VOD content can be created by examining unencrypted data representing digital content to identify segments of content for **encryption** ; **encrypting** the identified segments fo content using a first **encryption** method associated with a first conditional access system to produce second **encrypted** segments; and replacing the identified segments of content witht he first **encrypted** content and the second **encrypted** content in the digital content, to produce the multipe selectively **encrypted** VOD content.

French Abstract
...de contenu identifies a l'aide d'un second procede de cryptage associe a un **second** **systeme** d'acces conditionnel afin de produire des seconds segments cryptes; et a remplacer les segments...

Detailed Description
... of content to be encrypted that are important or critical to the decoding of the **content** , **duplicating** those selected **segments** **content** and encrypting each **copy** using a **different** **encryption** **method** (one for each CA system in use). The resulting multiple selectively encrypted content is then...

...understand that any time critical PCR information should be fixed along with the Continuity Counter **information** in the **duplicated** packets.

When VOID **content** is ordered by a subscriber at 214, the cable system (e.g., using registration information...

...what type of STB is associated with the order and thus what type of CA **encryption** **system** is being used by the ordering STB at 218. Once this is determined, there is...

22/3,K/32 (Item 32 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

01101351 **Image available**
CONTENT DISTRIBUTION FOR MULTIPLE DIGITAL RIGHTS MANAGEMENT
DISTRIBUTION DE CONTENU POUR GESTIONS DE DROITS NUMERIQUES MULTIPLES
Patent Applicant/Assignee:
SONY ELECTRONICS INC, 1 Sony Drive, Park Ridge, NJ 07656, US, US (Residence), US (Nationality)
Inventor(s):
CANDELORE Brant L, 10124 Quail Glen Way, Escondido, CA 92029-6502, US,
Legal Representative:
KANANEN Ronald P (et al) (agent), RADER FISHMAN & GRAUER PLLC, 1233 20th Street, NW, Suite 501, Washington, DC 20036, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200423717 A2-A3 20040318 (WO 0423717)
Application: WO 2003US27774 20030908 (PCT/WO US03027774)
Priority Application: US 2002409675 20020909
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ
EC EE EG ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK
LR LS LT LU LV MA MD MG MK MN MW MX MZ NI NO NZ OM PG PH PL PT RO RU SC

SD SE SG SK SL SY TJ TM TN TR TT TZ UA UG UZ VC VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL PT RO SE SI SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 6779

English Abstract
...Unencrypted data representing digital content is examined to identify at least segments of content for **encryption** (608). The identified **segments** of **content** are **duplicated** (610) and then encrypted using a first **encryption method** associated with a first DRM to produce first encrypted **segments** . **Duplicates** are encrypted using a **second encryption method** associated with a second DRM to produce second **encrypted segments** (614). A set of pointers are generated that point to the first and second **encrypted** segments content (618). A file is then created containing first and second **encrypted** segments of content (622). A file is then created containing first and second **encrypted** segments of content, pointers and unencrypted content along with DRM rights data to produce a selectively **encrypted** multiple DRM enabled file.

22/3,K/33 (Item 33 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

01035641 **Image available**
DECODING AND DECRYPTION OF PARTIALLY ENCRYPTED INFORMATION
DECODAGE ET DECHIFFREMENT D'INFORMATION PARTIELLEMENT CHIFFREE
Patent Applicant/Assignee:
SONY ELECTRONICS INC, 1 Sony Drive, Park Ridge, NJ 07656, US, US (Residence), US (Nationality)
Inventor(s):
UNGER Robert Allan, 2072 Vista Hermosa Way, El Cajon, CA 92019, US,
CANDELORE Brant L, 10124 Quail Glen Way, Escondido, CA 92029-6502, US,
PEDLOW Leo M Jr, 17193 Garjan Lane, Ramona, CA 92065, US,
Legal Representative:
KANANEN Ronald P (agent), RADER FISHMAN & GRAUER PLLC, 1233 20th Street, NW, Suite 501, Washington, DC 20036, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200365724 A1 20030807 (WO 0365724)
Application: WO 2002US40045 20021213 (PCT/WO US0240045)
Priority Application: US 200237498 20020102; CA 2406329 20021001
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SC SD SE SG SK SL TJ TM TN TR TT TZ UA UG UZ VC VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LU MC NL PT SE SI SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 20471

Fulltext Availability:
Detailed Description

English Abstract
An encryption arrangement for **multiple encryption** of television programs (100). A system according to embodiments of the present invention **multiple encrypts** only a portion of data (118,124) required for full presentation of a television program to permit coexistence of **multiple** conditional access **encryption** systems associated with multiple manufacturer's set-top boxes within a single system. By only...
...portion of the program (188,124), dramatically less bandwidth is consumed than the alternative of **multiple encryption** of all program data, thus permitting a larger number of programs to be carried over...

Detailed Description
... them to PIDs B and C respectively, so that they can be identified later for **encryption** under two **different systems** .

Preferably, the **duplicate** packets are inserted into the **data** stream adjacent one another in the location of the originally duplicated packet now with PID...

22/3,K/34 (Item 34 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2006 WIPO/Univentio. All rts. reserv.

01031187 **Image available**
CRITICAL PACKET PARTIAL ENCRYPTION
CRYPTAGE PARTIEL DE PAQUETS CRITIQUES
Patent Applicant/Assignee:
SONY ELECTRONICS INC, 1 Sony Drive, Park Ridge, NJ 07656, US, US (Residence), US (Nationality)
Inventor(s):
UNGER Robert Allan, 2072 Vista Hermosa Way, El Cajon, CA 92019, US,
CANDELORE Brant L, 10124 Quail Glen Way, Escondido, CA 92029-6502, US,
Legal Representative:
KANANEN Ronald P (agent), RADER FISHMAN & GRAUER PLLC, 1233 20th Street, NW, Suite 501, Washington, DC 20036, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200361289 A1 20030724 (WO 0361289)
Application: WO 2002US40050 20021213 (PCT/WO US0240050)
Priority Application: US 200238217 20020102; CA 2405901 20021001
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SC SD SE SG SK SL TJ TM TN TR TT TZ UA UG UZ VC VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LU MC NL PT SE SI SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 22404

Fulltext Availability:
Detailed Description
Claims

English Abstract
An encryption arrangement for **multiple encryption** of television programs. A system according to embodiments of the present invention **multiple encrypts** only a portion of the data required for full

presentation of a television program to...

...encrypting a portion of the program, dramatically less bandwidth is consumed than the alternative of **multiple encryption** of all program data, thus permitting a larger number of multiple conditional access systems in...

Detailed Description
... them to PIDs B and C respectively, so that they can be identified later for **encryption** under two **different systems** .

Preferably, the **duplicate** packets are inserted into the **data** stream adjacent one another in the location of the originally duplicated packet now with PID...

Claim
... packets into the digital content in place of the first duplicate packets to produce partially **encrypted** content. 129. The **method** according to claim 128, further comprising identifying the second duplicate packets and encrypting the second duplicate packets to produce second encrypted duplicate packets.
130. Themethodaccordingtoclaim129,furthercomprisinginsertingthesecond encrypted **duplicate** packets into the digital content in place of the second **duplicate** packets to produce partially dual **encrypted** content.
. A **method** of manipulating packetized digital content, comprising:
examining unencrypted packets to identify a predetermined packet type...

...packets; and
inserting the first and secondencrypted packets into the digital content to produce partially **encrypted** content. 132. The **method** according to claim 131, wherein the first and second duplicate packets are encrypted under first and second **encryption algorithms.\.**
. A **method** of manipulating packetized digital content, comprising:
examining unencrypted packets to identify a predetermined packet type...

...first and second duplicate packets;
encrypting the first duplicate packets; and
inserting the encrypted first **duplicate** packets into the digital **content** to produce partially **encrypted** content. . A **method** of allowing multiple conditional access providers in a content delivery system, comprising:
examining unencrypted packets...

...identify packets of a
predetermined type;
encrypting packets of the predetermined type using a first **encryption method** used by a first conditional access provider

22/3,K/35 (Item 35 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

01031186 **Image available**
PARTIAL ENCRYPTION AND PID MAPPING
CRYPTAGE PARTIEL ET MISE EN CORRESPONDANCE D'IDENTIFICATEURS DE PAQUETS
Patent Applicant/Assignee:
SONY ELECTRONICS INC, 1 Sony Drive, Park Ridge, NJ 07656, US, US (Residence), US (Nationality)
Inventor(s):
CANDELORE Brant L, 10124 Quail Glen Way, Escondido, CA 92029-6502, US,
UNGER Robert Allan, 2072 Vista Hermosa Way, El Cajon, CA 92019, US,
PEDLOW Leo M Jr, 17193 Garjan Lane, Ramona, CA 92065, US,
Legal Representative:
KANANEN Ronald P (agent), Rader Fishman & Grauer PLLC, 1233 20th Street,

NW, Suite 501, Washington, DC 20036, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200361288 A1 20030724 (WO 0361288)
Application: WO 2002US39958 20021213 (PCT/WO US0239958)
Priority Application: US 200237499 20020102; CA 2405899 20021001
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SC SD SE SG SK SL TJ TM TN TR TT TZ UA UG UZ VC VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LU MC NL PT SE SI SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 21149

Fulltext Availability:
Detailed Description
Claims

English Abstract
An encryption arrangement for **multiple** **encryption** programs. A system according to embodiments of the present invention **multiple** **encrypts** only a portion of the data required for full presentation of a television program to permit coexistence of **multiple** conditional access **encryption** systems (40, 140) associated with multiple manufacturer's set-top boxes (36, 136) within a single system. PID mapping techniques are used to distinguish between **multiple** encryptions. By only **encrypting** a portion of the program, dramatically less bandwidth is consumed than the alternative of **multiple** **encryption** of all program data, thus permitting a larger number of programs to be carried over...

Detailed Description
... them to PIN B and C respectively, so that they can be identified later for **encryption** under two **different** **systems** , Preferably, the **duplicate** packets are inserted into the **data** stream

Claim
... medium carrying encrypted content encrypted by the method according to claim 1 0.

30 A **method** of encrypting content, comprising:
encrypting content according to a first encryption method to produce a... method according to claim 33, further comprising encrypting the replicated identified portion using a first **encryption** **algorithm** .
1 0
1 1 35. The method according to claim 34, further comprising:
1 2...

...second
1 3 replicated portion; and
1 4 encrypting the second replicated portion using a **second** **encryption**
1 5 **algorithm** .
1 6
1 7 36. The method according to claim 35, further comprising combining the...encrypting a portion of the packets containing the digital television signal
according to a first **encryption** **algorithm** ;
encrypting the portion of the packets containing the digital television signal

according to a **second encryption algorithm** ;
leaving a **portion** of the packets containing the digital television signal
unencrypted;
assigning a primary packet identifier to...

...unencrypted packets;
assigning a primary packet identifier to the packets encrypted under the first
0 **encryption algorithm** ; and
assigning a secondary packet identifier to the packets encrypted under the 2 second encryption...

22/3,K/36 (Item 36 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

01031081 **Image available**
ELEMENTARY STREAM PARTIAL ENCRYPTION
CRYPTAGE PARTIEL DE TRAINS DE DONNEES ELEMENTAIRES
Patent Applicant/Assignee:
SONY ELECTRONICS INC, 1 Sony Drive, Park Ridge, NJ 07656, US, US (Residence), US (Nationality)
Inventor(s):
CANDELORE Brant L, 10124 Quail Glen Way, Escondido, CA 92029-6502, US,
UNGER Robert Allan, 1072 Vista Hermosa Way, El Cajon, CA 92019, US,
PEDLOW Leo M Jr, 17193 Garjan Lane, Ramona, CA 92065, US,
MIRSKY Gregory, 3048 Stelling Drive, Palo Alto, CA 94303, US,
EYER Mark Kenneth, 15601 133rd Place, N.E., Woodinville, WA 98072, US,
Legal Representative:
KANANEN Ronald P (agent), Rader Fishman & Grauer PLLC, 1233 20th Street, NW, Suite 501, Washington, DC 20036, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200361173 A2-A3 20030724 (WO 0361173)
Application: WO 2002US40051 20021213 (PCT/WO US02040051)
Priority Application: US 200237914 20020102; CA 2405865 20021001
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SC SD SE SG SK SL TJ TM TN TR TT TZ UA UG UZ VC VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LU MC NL PT SE SI SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 19125

Fulltext Availability:
Detailed Description

English Abstract
An encryption arrangement (108) for **multiple encryption** of television programs. A system according to the embodiments of the present invention **multiple encrypts** only a portion of the data required for full presentation of a television program to permit coexistence of **multiple** conditional access (118 and 124) **encryption** systems associated with multiple manufacturer's set-top boxes (36 and 136) within a single...

...encrypting a portion of the program, dramatically less bandwidth is

consumed than the alternative of **multiple encryption** of all program data, thus permitting a larger number of programs to be carried over...

Detailed Description
... selects packets that are to be dual encrypted under any of the above partial dual **encryption methods** . Those packets are then duplicated with new PIDs so that they can be later identified...

...them to PIDs B and C r6gjYectively, so that they can be identified later for **encryption** under two **different systems** .

Preferably, the **duplicate** packets are inserted into the **data** stream adjacent one another in the location of the originally duplicated packet now with PID...

22/3,K/39 (Item 39 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

01006414 **Image available**
SECURED DIGITAL SYSTEMS AND A METHOD AND SOFTWARE PRODUCT FOR OPERATING THE SAME
SYSTEMES NUMERIQUES SECURISES ET PROCEDE ET LOGICIEL POUR LES FAIRE FONCTIONNER
Patent Applicant/Assignee:
SECURED DATA SYSTEMS LLC, 149 McCloy Road, Beaver Falls, PA, US, US (Residence), US (Nationality)
Inventor(s):
TOWER James Brian, 2048 Lara Court, Tracy, CA, US,
CHUMURA Sean David, 700 Speyer Avenue, Monaca, PA, US,
Legal Representative:
WESTERHOFF Richard V (agent), Eckert Seamans Cherin & Mellott, LLC, 600 Grant Street, 44th Floor, Pittsburgh, PA 15219, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200336480 A2-A3 20030501 (WO 0336480)
Application: WO 2002US33536 20021021 (PCT/WO US02033536)
Priority Application: US 2001999786 20011023
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ
EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR
LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI
SK SL TJ TM TN TR TT TZ UA UG UZ VC VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LU MC NL PT SE SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 14970

Fulltext Availability:
Detailed Description

English Abstract
...been compromised, such as by a malicious attack or corrupted data. The file units remain **encrypted** except during processing with successive generations of each **encrypted** file unit stored in a secured memory, which cannot be overwritten but only copied. Compromised...

...is reduced by frequent optimization of system operation. Digital systems only accept file units from **other** secure digital **systems** having an

approved digital identifier, which is embedded in each file unit.

Detailed Description
... code set to determine a best match from a plurality of potential best character code **matches** . For **text** based **file** units, a spell-cbeck, dictionary check and graminar check can be used to assist in determining the best character code **match** , or when the **file** units are expressed in hexadecimal code, a substitute hexadecimal code can be used which produces...encrypted and remain encrypted except during processing. Not only is the data element of a **file** unit encrypted but also the tag **elements** using a **separate encryption key** . The tag unit requires decryption before the **data element** can be decrypted as the tag contains the key for the data element encryption.

Yet...7, the tag 31 of the file unit is decrypted at 81 using a first **encryption key** . As mentioned, the tag includes a **second** encryption **key** which is used at 83 to decrypt the **data element** of the file unit. If the file unit was not
15
copied from the secured...unique file ID) in the memory map at 99, 101 and 103. If the tag **elements match** those in the memory map at 105, then the file unit is considered to be...

22/3,K/40 (Item 40 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2006 WIPO/Univentio. All rts. reserv.

00945799 **Image available**
TRUSTED AUTHORIZATION DEVICE
DISPOSITIF D'AUTORISATION SECURISE
Patent Applicant/Assignee:
ENTERPRISES SOLUTIONS INC, 1040 Wood Road, Suite 200, Braintree, MA 02184 , US, US (Residence), US (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
MICHENER John R, 1740 Merlot Way, Salinas, CA 93906, US, US (Residence), US (Nationality), (Designated only for: US)
RYAN Paul F, 821 Smartts Lane, Leesburg, VA 20176, US, US (Residence), US (Nationality), (Designated only for: US)
Legal Representative:
VAN VOORHIES Kurt L (agent), P.O. Box 68, DeTour Village, MI 49725, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200279960 A1 **20021010** (WO 0279960)
Application: WO 2002US10353 20020401 (PCT/WO US0210353)
Priority Application: US 2001280090 20010330
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ
EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR
LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI
SK SL TJ TM TN TR TT TZ UA UG US UZ VN YU ZA ZM ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 9391

Patent and Priority Information (Country, Number, Date):
Patent: ... **20021010**
Fulltext Availability:
Claims

English Abstract
...of the TAD (10); generates (212) a signature of the second information using a first **encryption** process; egnerates (216) a set of session keys (Ks1, Ks2, Ks3) by a **second encryption process** responsive to the random number (R) and a set of stored working keys (K"sub"w1, K"sub"w2, K"sub"w3); and generates (218) third information by **encrypting** the second information and the signature using a third **encryption** process responsive to the set of session keys (Ks1, Ks2, Ks3). A dat structure (42...
Publication Year: **2002**

Claim
... is responsive to said first identification code;
c. providing for generating a set of session **keys** by a second encryption **process** , wherein said second **encryption process** is ... for generating second information and fifth information by decrypting said third information using said third **encryption process** that is responsive to said set of
session keys;
e. providing for generating a signature of said second information, wherein said
signature is generated by said first **encryption process** ;
f. providing for comparing said signature with said fifth information; and g. if said signature...further comprising providing for transmitting to a third computer said random number, a set of **encrypted** working keys for said third **encryption process** and said third information, and receiving from said third computer a result, wherein said set of **encrypted** working **keys** is responsive to said first identification code, said set of **encrypted** working **keys** are **encrypted** with a set of keys of said third computer, the operation of providing for acting...

22/3,K/41 (Item 41 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00944776 **Image available**
DATA PROTECTION SYSTEM THAT PROTECTS DATA BY ENCRYPTING THE DATA
SYSTEME DE PROTECTION DE DONNEES PROTEGEANT LES DONNEES PAR CHIFFREMENT DE CELLES-CI
Patent Applicant/Assignee:
MATSUSHITA ELECTRIC INDUSTRIAL CO LTD, 1006, Oazakadoma, Kadoma-shi, Osaka 571-8501, JP, JP (Residence), JP (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
NAKANO Toshihisa, 3-35-15, Shimeno, Neyagawa-shi, Osaka 572-0077, JP, JP (Residence), JP (Nationality), (Designated only for: US)
OHMORI Motoji, 9-3-402, Nasuzukuri 1-chome, Hirakata-shi, Osaka 573-0071, JP, JP (Residence), JP (Nationality), (Designated only for: US)
MATSUZAKI Natsume, 1-6-7-803, Aomadaninishi, Minou-shi, Osaka 562-0023, JP, JP (Residence), JP (Nationality), (Designated only for: US)
TATEBAYASHI Makoto, 1-16-21, Mefu, Takarazuka-shi, Hyogo 665-0852, JP, JP (Residence), JP (Nationality), (Designated only for: US)
Legal Representative:
NAKAJIMA Shiro (agent), 6F, Yodogawa 5-Bankan, 2-1, Toyosaki 3-chome, Kita-ku, Osaka-shi, Osaka 531-0072, JP,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200278419 A2-A3 **20021010** (WO 0278419)
Application: WO 2002JP3055 20020328 (PCT/WO JP0203055)
Priority Application: JP 200195730 20010329; JP 2001285608 20010919
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ

EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS KE KG KP KR KZ LC LK LR LS
LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK
SL TJ TM TN TR TT TZ UA UG US UZ VN YU ZA ZM ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 28452

Patent and Priority Information (Country, Number, Date):
Patent: ... **20021010**
Fulltext Availability:
Detailed Description

English Abstract
The present invention is a data protection system that includes a **multiplicity** of terminals, and an **encryption** device that **encrypts** distribution data that is distributed to each terminal. Each terminal is corresponded with one node...
Publication Year: **2002**

Detailed Description
... software,- or the like for decrypting digital content using the exposed key, and make illegal **copies** of the digital **content** . Consequently, to protect copyright it will no longer be possible to encrypt and distribute digital content using an **encryption key** that corresponds to the exposed decryption key.

For example, taking into consideration a DVD reproductionresult, after the master key is exposed, DVD manufacturers must use a **different** master **key** to **encrypt** digital **content** for distribution. However, a problem arises that since the DVD reproduction terminal that has been...

22/3,K/42 (Item 42 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00929774 **Image available**
METHOD AND APPARATUS FOR PARTIAL ENCRYPTION OF CONTENTS
PROCEDE ET APPAREIL DE CHIFFREMENT PARTIEL DE CONTENUS
Patent Applicant/Assignee:
HEWLETT-PACKARD COMPANY, 3000 Hanover Street, Palo Alto, CA 94303-1881, US, US (Residence), US (Nationality)
Inventor(s):
HERLEY Cormac, 24420 Big Basin Way, Los Gatos, CA 95033, US,
YU Yihong, 31-6 Briarwood Lane, Marlborough, MA 01752, US,
Legal Representative:
HEMINGER Susan E (agent), Hewlett-Packard Company, Legal Department, IP Section, P.O. Box 272499, Ft. Collins, CO 80527-2400, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200263852 A2-A3 **20020815** (WO 0263852)
Application: WO 2002US3862 20020205 (PCT/WO US0203862)
Priority Application: US 2001776680 20010206
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ
EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR
LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI
SK SL TJ TM TN TR TT TZ UA UG UZ VN YU ZA ZM ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR

(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 3624

Patent and Priority Information (Country, Number, Date):
Patent: ... **20020815**
Fulltext Availability:
Detailed Description

English Abstract
The present invention is directed to methods and apparatus that partially **encrypt** an information data file. An exemplary method includes dividing (210) the information file into a...

...information file to preclude reconstruction of the information file using only the first file, and **encrypting** (215) the **second** file. Additionally, the **method** provides for transmitting the first file and the **encrypted** second file from a first device (510) to a second device (530).
Publication Year: **2002**

Detailed Description
... embodiment, the image file 340 is not available outside the secure device 360. Therefore, a **copy** of the **image file** 300 is not available for
unauthorized copying by the owner of the device 360. The **encryption** /decryption **process** can include additional use limitations, such as limiting the number of prints that can be made from the reconstructed image file 340.

2 5 The division of the **information file** can be accomplished by any of
different methods . For example, **parts** of the **information file** that form the second file can be selected by a user selected pattern or from...

22/3,K/43 (Item 43 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2006 WIPO/Univentio. All rts. reserv.

00857633 **Image available**
A HYBRID STREAM CIPHER
CHIFFREMENT A CHAINE HYBRIDE
Patent Applicant/Assignee:
MAINSTREAM ENCRYPTION, 2835 E. Washington Boulevard, Los Angeles, CA 90023, US, US (Residence), US (Nationality)
Inventor(s):
ANANTH Viswanath, 27127 Candington Court, Valencia, CA 91354, US,
Legal Representative:
SCHAAL William W (et al) (agent), Blakely, Sokoloff, Taylor & Zafman, 7th floor, 12400 Wilshire Boulevard, Los Angeles, CA 90025-1026, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200191367 A1 **20011129** (WO 0191367)
Application: WO 2001US16931 20010523 (PCT/WO US0116931)
Priority Application: US 2000206605 20000523; US 2001864042 20010522
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ
EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR
LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL

TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 22063

Patent and Priority Information (Country, Number, Date):
Patent: ... **20011129**
Fulltext Availability:
Detailed Description

English Abstract
In one embodiment, a hybrid stream **cipher** operating within a computing device. The hybrid stream **cipher** comprises at least two software routines. A first routine (155) is responsible for dividing incoming plain text into variable-sized blocks (105). A **second** software **routine** is for converting the plain text into **cipher** text based on an **encryption** key (115), an internal identifier and perhaps a percentage of random data value (100).
Publication Year: **2001**

Detailed Description
... cipher text sequence.

Another feature introduced by the hybrid stre'am cipher i:nvolves a **second** verification and decryption **routine** which includes decrypting "COUNT' cipher **text** , removing "TAIC'random **data** , and verifying the hash bytes in cipher text stream (see item 1027). The details of...

...LENGTH. Next, the combined stream data (including cipher text and hash bytes) and the random **data** are separated in the data sequence. Then, the **second** verification **routine** decrypts the **cipher** **text** at the positions previously identified, **copies** the hash bytes into the array HASH-BYTES[and initializes the hash byte positions in...